BCAP NewsClips

February 25, 2019

Light Reading
Verizon Appears to Walk Back 5G Home Buildout Goal

Fierce Video
How Batman is helping prove out 5G, cloud-based mixed reality

USA Today
Sprint's 5G network will go live this May in Chicago, Atlanta, Dallas and Kansas City

CNBC
Trump is right that the US risks losing the 5G race, Huawei chairman says

Fierce Video
Verizon to launch mobile 5G service in 30 markets this year

CNN
Apple needed a kick in the pants. Samsung just delivered it

Philadelphia Daily News
As 2020 Democratic candidates line up, who's most likely to appeal to Pa.?

Privacy would seem a big thing for consumers, given recent events. **Class action lawsuits** against tech firms, noise about **privacy legislation**, and a new demand for **privacy related jobs** are all signs that keeping information confidential has become important.

So it's not surprising that a **privacy survey** from IBM's Institute for Business Value that came out Monday would show some big reactions to the topic, as Axios reported. Eighty-one percent of consumers say they've become more concerned about how companies use their data, while 87% think companies should be more heavily regulated on personal data management. Three-quarters of the people felt like they were less likely to trust companies with data and 89% said companies should be clearer about how their products use data.

But even though consumers are concerned with one story after another of companies losing or misusing personal data, apparently it's not enough for them to take actions in response. Seventy-one percent said that they were willing to give up privacy to get access to what technology can offer. Only 45% have updated their privacy settings on products in response and 16% walked away from a company because of data misuse. It's already been clear that one reasons for big data leaks is because there is **little financial risk** to companies, as Motherboard reported. This new data suggests that companies have even less to worry about, as most people are willing to keep doing business with them. – ***Fortune***

Popular health and fitness apps scrambled to stop sending sensitive personal information to Facebook Inc. after ***The Wall Street Journal* reported** Friday many were transmitting detailed information about topics including their users' weight and menstrual cycles.

Since Friday, at least four of the apps that the Journal had identified and contacted as part of its reporting issued updates to cut off transmission of sensitive data to Facebook, a new round of testing showed Sunday. **The apps that made the change** include Flo Health Inc.'s Flo Period & Ovulation Tracker and Azumio Inc.'s Instant Heart Rate: HR Monitor, the tests showed. Another popular food- and exercise-logging app, Lose It!, from FitNow Inc., also stopped sending

Pennlive
Pa. election officials took freebies from voting machine companies: audit

Facebook information, Sunday's test showed. In a test on Thursday, the app had been sending Facebook the weight users logged, along with how much they had gained or lost and the caloric content of every food item they logged.

The changes came as Facebook itself contacted some large advertisers and developers in response to the Journal's reporting, telling them it prohibits partners from sending Facebook any sensitive information about users. The company said it is working on new systems to detect and block uploads of such information by apps, according to a person whose company was contacted by Facebook. In at least one message, Facebook directed a major developer to ensure that it had a legal justification for all the user information it sends Facebook in its app via the software-development kit, or SDK, the social network provides for apps, the person said. "We work with the app developers using our SDK to ensure they adhere to our terms. In cases where we see violations, we work with the app developers to get into compliance and take action as needed," a Facebook spokeswoman said.

A spokeswoman for Flo Health confirmed Sunday that it had deleted Facebook's software from its app and requested that Facebook delete all the user data it had previously sent. Azumio and FitNow didn't respond to requests for comment on Sunday. The Journal's testing showed that at least 11 popular apps were using software that Facebook provides to app developers to send the social network intimate information. The Facebook analytics service the apps used allowed their developers to see the sensitive data in an aggregated form—and target their users with ads on Facebook based on that information.

Facebook has said that it doesn't otherwise use that type of app data, although the company's business terms of service give it latitude to do so. The sensitive information was shared with Facebook regardless of whether the app user was a member of the social network, the testing showed. New York Gov. Andrew Cuomo on Friday ordered state agencies to investigate apps' transmission of personal information to Facebook described in the Journal report and urged regulators in Washington to look into the matter as well. In Washington, D.C., Sen. Ed Markey, a Democrat from Massachusetts, called the behavior "a new low in privacy malpractice."

In the U.K., Damian Collins, chairman of the House of Commons Digital, Media, Culture and Sport Committee, which last week called for more regulation of social media, **said on Twitter** that the Journal's reporting "shows how totally out of control the system is." The sharing of such intimate data with Facebook provoked a discussion about who is responsible for data shared via SDKs that are built into nearly all mobile applications. Facebook's is one of the most popular SDKs, but the average app on Apple Inc.'s iOS includes 19, according to app-analytics firm Apptopia.

Those kits help developers integrate certain features or functions, such as analytics tools like Facebook's, that allow apps to better understand their users' behavior or to collect data to sell targeted advertising. SDKs at times send detailed information on what users do inside apps to third parties—some of whom are bound by strict contracts never to use the information, and others which aren't. A Facebook

spokeswoman said that such data sharing is “industry-standard practice.”

Some in the tech industry said that Facebook wasn’t responsible for the data sharing, even if it built the SDK, because developers decided what data they share with the company using the tool, and it would be impossible for the company to effectively police what it is sent. Others said Facebook should assume responsibility for a system it helped build. “Every part of this data chain will say, ‘oh look at some other part is doing this or that.’ They’re all correct,” Zeynep Tufekci, an associate professor at the University of North Carolina, Chapel Hill, **said on Twitter**. “The whole surveillance-industrial complex is corrupt and its mechanisms aren’t clear to ordinary people.” – ***Wall Street Journal***

BCAP
Broadband
Cable Association
of Pennsylvania
127 State Street Harrisburg, PA 17101
717-214-2000 (f) 717-214-2020
bcapa.com
First in Broadband.
The Future of Broadband.®